UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/706,954	11/14/2003	Osamu Asano	122.1571	7775

21171   7590   05/22/2008
STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>25 February 2008</u>.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☐ Claim(s) <u>1,3-7,9-15,17 and 20</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) <u>1, 3-7, 9-15, 17 and 20</u> is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☒ All b) ☐ Some * c) ☐ None of:
        1. ☒ Certified copies of the priority documents have been received.
        2. ☐ Certified copies of the priority documents have been received in Application No. _____.
        3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
           application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date <u>1/03/08</u>
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth
   in 37 CFR 1.17(e), was filed in this application after final rejection. Since this
   application is eligible for continued examination under 37 CFR 1.114, and the fee set
   forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action
   has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on
   2/25/08 has been entered.

Response to Arguments

2. In light of applicant's arguments and amendments the previously cited 35 USC § 112
   rejections are withdrawn.

3. *Applicant argues that Campbell does not disable transmission of the data to [all] the*
   communication devices other than the communication device that transmitted the
   infected data because Campbell disables sending the virus packet to the intended
   computer and does not disable sending the virus packet to <u>all</u> the computers".
   The examiner points to Campbell's paragraph [0005], which teaches that the
   received packets "are forwarded to the destination port <u>only</u> if they are free of virus
   signatures or any virus attack pattern" and Campbell does not teach transmitting the
   received packets to computers other than the data is directed to (the destination),
   but the invention aims to provide protection against virus attacks based on the
   identified infected packets and clearly forwarding the infected data to other
   computers would be against the principle of the problem that Campbell attempts to
   solve.

Additionally, the examiner points out that the limitation of "disabling sending the virus

packet to <u>all</u> computers connected to a network" is present only in claim 20 (and not

in claim 1, for example, that applicant argues).

4. *Applicant argues that the newly introduced limitation: "the virus preventing unit*

registers a transmission MAC address of a communication device that transmitted

the [infected] data to the hub unit" is not found in Campbell.

This newly introduced limitation is address in this Office Action, below.

5. *On pg. 8 paragraph 2-3 applicant appears to address differences between IP and*

MAC addressing scheme.

However, applicant argument is not clear and, as a result, at this point the examiner

points out that although IP address is widely used in the network communication

(e.g. in TCP/IP protocol), the hardware (MAC) address is <u>necessary</u> for data delivery

in the network environment (such as LAN utilizing hubs, for example).

6. NOTE: although Masatoshi's invention, cited in the previous Office Action, remains

to be relevant to applicant claim language, for purpose of simplicity the art is not

used in the current rejection.

7. Claims 1, 3-7, 9-15, 17 and 20 have been examined.

The text of those sections of Title 35, U.S. Code not included in this action can be

found in a prior Office action.

Information Disclosure Statement

The information disclosure statement filed on 1/3/08 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Rejections - 35 USC § 103

8. Claim 20 is rejected under 35 U.S.C. 103(a) as obvious over Milliken (USPUB 20030115485) in view of Kim (USPN 2002/0010869) or alternatively in view of Bhogal (USPN 7248563).

Milliken (USPN 2003/0115485) teaches hash based system for detecting and preventing the transmission of malicious packets, such as worms and viruses (Milliken, [0003]). Milliken discloses detecting data infected with a virus based on virus patterns stored in a storage unit (malicious pattern rules utilized by an algorithm to detect malicious traffic, see Milliken [0029-30], Fig. 4 A and B etc.) and disabling transmission of the data infected with the virus to all computers connected to a network by blocking communication between the network and a computer that transmitted the data infected with the virus based on the address of the computer (Milliken [0030]).

9. Milliken does not disclose that the blocking is based on MAC address.

Kim discloses blocking based on MAC address (e.g. Kim, col. [0018]). Alternatively, Bhogal discloses blocking based on MAC address (e.g. col. 8 lines 1-23).

It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to use MAC address to block data as disclosed by Kim, or alternatively by

Bhogal, given the benefit of increased security (e.g. eliminate possibility of spoofing).

10. Claims 1, 3-5, 9-10, 12-15, 17 and 19-20 are rejected under 35 U.S.C. 103(a) as

obvious over Campbell (USPN 20040003284) in view of Lim (USPUB

2005/0010814) and further in view of Kim (USPN 2002/0010869) or, alternatively,

Bhogal (USPN 7248563).

Campbell discloses a hub system (Fig. 2 object 72) performing monitoring data for

viruses in "on-line" mode.

11. As per claims 1, 15, 17 and 20, Campbell discloses a hub unit comprising a first

memory unit storing virus pattern information (virus database 100 disclosed in Fig.

2), a second memory unit temporarily storing data received from any one of the

communication devices (e.g. packet queue 122), a virus detecting unit that

determines whether the data temporarily stored in the second memory unit is

infected with a virus or not based on the virus patterns stored in the first memory unit

(e.g. virus scanner 126) and a virus spreading preventing unit (e.g. switching control

78) that disables, when the virus detecting unit detects infected data, transmission of

the data outside the hub unit to the communication devices directly connected to the

hub unit, other than a communication devices that transmitted the infected data (as

indicated in paragraph [28] disclosing shutting off the port on which the infected

computer is connected to prevent any further spreading of the virus to any device

and as explicitly taught in paragraph [5], the received packets "are forwarded to the

destination port <u>only</u> if they are free of virus signatures or any virus attack pattern,
Campbell [0005])).

Even if Campbell did not teach disabling the transmission of the infected data
outside the hub unit to the communication devices, blocking/discarding infected
packets would have been an obvious variation well known in the art (e.g. Libenzi
USPN 6993660), and an ordinary artisan would have been motivated to implement
such solution given the benefit of preventing spread of viruses.

12. Campbell does not teach registering a transmission address of a communication
device that transmitted the data to the hub unit in a (third) memory transmission
addresses of the plurality of the communication devices when the virus detecting
unit determines that data is infected with a virus.

13. Lim discloses registering an address in memory after the virus is found (Fig. 2, e.g.
element 120-125, and associated text). It would have been obvious to one of
ordinary skill in the art at the time of applicant's invention to configure a virus related
entity such as the virus spreading preventing unit to register an address of a
communication device that transmitted the infected data to the hub unit in order to
imposed a predetermined policy (e.g. blocking time) to the infected address.

14. Campbell in view of Lim does not disclose that the address is a MAC address.
Kim discloses use of (blocking based on) MAC address (e.g. Kim, col. [0018]).
Alternatively, Bhogal discloses the use of MAC address (e.g. col. 8 lines 1-23).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use MAC address as disclosed by Lim or alternatively by Bhogal to increase security (e.g. eliminate possibility of spoofing).

15. As per claim 3, Cambell, disabling transmission is not limited to only previously received data from a first communication device. Furthermore, the previously received data at some point must have been a newly received data. Lastly, as discussed above, Cambell discloses preventing transmitting data received on the port from the "infected" communication device. Thus, any following data will also be prevented from reaching other communication devices, which reads on claim 5.

16. As per claims 4 and 9-10, preventing newly received data from a first communication device to the communication devices reads on disabling the reception of new data from a first communication device.

17. As per claims 13-14, although Cambell call his system implementing monitor functionalities a router [5]), Cambell is silent in regard to the monitor to be (implemented in) a gateway. However, the examiner points out that the hub/switch/router/gateway systems have essentially similar functionalities (the data is communicated through the system from a source to a destination) and given the fact that gateways are old and well known in the art of networking (see USPUB 2004/0047356, for example), an ordinary artisan would have been motivated to include Campbell's monitor in systems such as gateway given the benefit of scanning network packets communicating through the gateway for viruses and as a result preventing possible virus attacks.

18. As per claim 12, although Campbell is silent regarding using more than one protection device, such as discussed above hub, being connected in a cascade form, the examiner points out that connecting plurality of protection devices in a cascade mode is well known in the art of computer networking (e.g. Fig. 1, Smith USPN 7134142), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to connect more than one protection device (in a cascade form) given the benefit of a multiple layer network protection.

19. Claims 6 and 11 are rejected under 35 U.S.C. 103(a) as obvious over Campbell (USPN 20040003284) in view of Lim (USPUB 2005/0010814) and Kim (USPN 2002/0010869), or alternatively Bhogal (USPN 7248563), and further in view of Togawa (U.S. Patent No. USPN 6240530).

Campbell system has been discussed above.

20. Campbell does not disclose a display unit for notifying that data is infected with a virus if the detecting unit determines that the data is infected with a virus.

Togawa discloses a display unit for notifying that data is infected with a virus if the detecting unit determines that the data is infected with a virus (Fig. 3 object 7, col. 24 lines 37-43 and col. 23 lines 9-15, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the display unit as disclosed by Togawa into Campbell in view of Lim and Kim, or alternatively Bhogal's invention given the benefit of alternative means of system's operator notification.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Norman (USPUB 2004/0088564),

Levin (USPUB 2003/0154394).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PETER POLTORAK whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Peter Poltorak/

Examiner, Art Unit 2134

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134